RETAIL EFT (ATM AND POS) WORKPROGRAM

CHAPTER 20WP

(FILE NAME ON DISK # 3 = IS-WP#15.WPD)

COMMENTS

This chapter is intended to determine the adequacy of controls over the retail EFT environment. The examiner must review compliance with established policy, the effectiveness of contingency/recovery planning, and assess the soundness of physical and internal controls. The reviews of work flows and control points will ensure that adequate control procedures have been established to maintain the accuracy and integrity of the data. The procedures are created, so that they may be implemented separately as part of either the IS examination or safety and soundness examinations. The examiner should document any findings, especially those which do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook*.

Tier I

RETAIL ELECTRONIC FUNDS TRANSFER (EFT) SYSTEMS

1. Obtain a description of each retail EFT related system operated by the institution, considering:

   a. Automated Teller Machines (ATM).
   b. Point-of-Sale (POS).
   c. Debit and/or Smart Cards.
   d. Home banking.

2. Review procedures employed for each EFT related service to ensure the integrity of plastic card and personal identification number (PIN) processing, including separation of functions over issuance of the cards, issuance of PINs, storage of cards and maintenance of software controlling PINs. The review should focus on controls that could lead to widespread misuse and significant losses to the institution.

3. Review a sample of agreements for each EFT related service to ensure that they adequately set forth responsibilities and liabilities of the institution and the customer, primarily as to requirements of the Electronics Funds Transfer Act (Regulation E).

4. Determine that a viable and tested contingency plan is in effect. The plan should provide for short-term recovery of data in-process, security, confidentiality of customer data, and reasonable time frames for full recovery, in relation to the volume and importance of the application to the institution's operation.

5. If applicable, review agreements with other switch or network operators to ensure each party's liabilities and

responsibilities are clearly defined, especially in the areas of settlement, security and confidentiality, and contingency processing.

6. Compare the last executed internal audit procedures covering each EFT related operation to the related questions detailed in Tier II of these procedures, and determine whether they meet or exceed Tier II coverage.

7. Determine that the audit function periodically performs an inventory of all EFT stations owned or operated by the institution and that each location is included in the audit program, either directly or indirectly (e.g., as part of a branch audit).

8. Review all audit reports covering any EFT related operation determine the current status of any exceptions noted in the audit report.

9. Procedures included in Tier II that are not sufficiently covered under steps 6 and 7, must be implemented in this examination. (Note: To the extent coverage is clearly satisfactory and current, audit procedures and workpapers may also be utilized to address steps 2 through 5).

CONCLUSIONS

10. Review the results of work performed in this chapter and in the chapters for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

11. Discuss with management:

    a. Violations of law, rulings, regulations, or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

	Comments
12. Assign rating, (see Chapter 5 for additional information).	
13. Prepare an index of workpapers for this section of the workprogram.	
14. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.	
15. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.	

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

(Note: Includes automated teller machines (ATM), point of sale (POS), debit/smart cards and home banking. To the extent the operations are autonomous, applicable questions should be applied separately for each application.)

ACCOUNTING AND PROCESSING

1. Are all general ledger accounts related to retail EFT reconciled on a timely basis?

2. Is each EFT system and origination site reconciled daily and are reconciling items adequately controlled?

3. Are reconcilements and exception items regularly reviewed by supervisory personnel?

4. If the institution is a participant in any shared EFT networks, is daily settlement with each network current and are reconciling items adequately controlled?

5. Are separate accounts used to control adjustments, unposted items, rejects, etc. and are they periodically reconciled?

6. For input reconstruction, are transactions files duplicated or otherwise retained for a minimum of 60 days as required by Regulation E to identify unauthorized transactions?

7. Is a separate investigation unit in place to control customer inquiries, unposted items, rejects, differences, etc., and do they periodically generate reports of outstanding items and aging for management?

8. Are exception reports (e.g., unposted items, rejects, differences, and aging of open items) receiving appropriate attention?

9. Is separation of duties maintained throughout each Retail EFT accounting process including receipt of transactions, file updates, adjustments, internal reconcilement, preparation of general ledger entries, posting to customers accounts, investigations, and reconcilement with network processors?

10. Are adjustments (e.g., changes to deposits and reversals) to original retail EFT instructions received by an individual that does not have access to the data or customer files?

PERSONAL IDENTIFICATION NUMBERS (PIN)

11. Is access to PIN data and operations completely removed from functions preparing or issuing plastic cards?

12. Are new PINs entered into the system by personnel who do not open accounts or have access to customer account information?

13. If issuance of a new PIN is necessary, have control procedures been established and is there accountability to the individual initiating such a transaction?

14. Are PINs issued in an environment that precludes matching them to customer account numbers or access forms (e.g., plastics)?

15. Is access to a customers account restricted after a small series (e.g., three) unsuccessful attempts to enter the correct PIN?

16. Are PINs encrypted or otherwise disguised when stored on computer files or transmitted over telecommunications lines?

17. Do procedures prohibit PIN information from being released via telephone?

18. If access to PINs maintained on computer files must be accessed for maintenance purposes, are activities closely supervised and is each occasion logged?

19. When selecting PINs, are customers discouraged from using common words or sequences numbers and words or numbers that can easily identify the customer?

PLASTIC CARDS

20. Are all retail payment cards:

    a. Issued only as required?

    b. Kept in a locked, secure location under dual-control?

    c. Controlled by access logs?

    d. Periodically inventoried?

	Comments
21. Are blank cards kept under effective dual control and accounted for in each of the various steps in encoding, embossing and mailing?	
22. Is access to the physical area in which encoding is performed restricted from access by unauthorized personnel?	
23. Is the working supply of plastics stored in a secure environment?	
24. Is use of encoding equipment well controlled?	
25. If cards are issued at more than one location (e.g., branches), have accountability and card control procedures been established for each location?	
26. Are cards mailed to customers in envelopes with a return address that does not identify the institution?	
27. Are returned cards controlled and accounted for by individuals who do not issue cards or have systems/operations responsibilities?	
28. Is it against policy for the institution to mail unsolicited cards?	
29. Are cards which were captured or inadvertently left at EFT terminal locations properly controlled?	
30. Are plastic cards and PINs always mailed separately and with a sufficient period of time between mailings?	
31. After a card is issued, is there follow-up to ascertain whether both card and PIN were received/utilized by the proper customer?	
32. Are procedures such as hot card lists and expiration dates used to limit the period of exposure if a card is lost, stolen or purposely misused?	
33. Are spoiled cards destroyed under dual control and are records maintained of all destroyed cards?	
34. Are test or demonstration cards adequately controlled?	
35. Are satisfactory controls maintained over any duplicate cards which were not issued to the customer (e.g., temporary access)?	

36. If vendors are employed to produce cards, have reviews been conducted by the institution or for the institution (e.g., third party or cooperatively with other users of the vendor) that meet or exceed the measures noted under PINs and Plastic Cards, above, as applicable?

OPERATIONAL CONTROLS

37. Are ATM data entry personnel prohibited from originating entries for processing or physically handling cash?

38. Is proper control of source documents (e.g. checks for deposit) maintained throughout the daily processing cycle relative to the following aspects:

    a. Input preparation?

    b. Reconcilement of item counts and totals?

    c. Output distribution?

    d. Storage of the instruments?

39. Are terminal and operator identification codes used for all types of retail EFT transactions?

40. Does the system prevent customer charges from exceeding the available balance in the account and/or approved overdraft lines?

41. Are access to and use of terminals used to change customer credit lines and account information adequately controlled?

42. Are retail EFT equipment keyboards and/or display units properly shielded to avoid disclosure of customers IDs or PINs?

43. Do customers receive a receipt showing the amount, date, time and location for retail EFT transactions?

44. Is each retail EFT transaction assigned a sequence number and terminal ID to provide an audit trail?

45. Are hot card or customer suspect lists regularly updated and distributed to each user location?

46. Is each home banking customer required to pre-authorize payments to specific merchants and/or transfers between accounts?

47. Are verification procedures in place for telephone instructed payments or transfers and are confirmations promptly sent to customers and merchants?

48. Are security devices and procedures for each EFT facility adequate?

49. Are merchants prohibited from accessing customer accounts or account information?

50. Are tests of program changes to retail EFT applications adequately controlled and are logs maintained for each test showing purpose and results?

51. Are software and equipment maintenance personnel closely supervised and are their activities logged?

AGREEMENTS/CONTRACTS

52. If the institution is a participant in any shared EFT network, do the written agreements between/among participants and operators of the network clearly set forth the rights and responsibilities of all parties, including security and confidentiality of customer information, settlement terms, contingency operations, and requirements for installing and servicing equipment and software?

53. Are agreements in effect with all vendors supplying services for retail EFT operations (e.g., plastic cards, equipment/software maintenance or ATM cash replenishment) that clearly define the responsibilities of both the vendor and the institution and do they provide for minimum control standards, the ability of the institution to audit the vendors operations, periodic submission of financial statements to the institution and contingency plans?

54. Are agreements in effect with all customers for each retail EFT service provided by the institution and do the agreements set forth the responsibilities and limits of liability of both the customer and the institution and do they include provisions of the Electronic Funds Transfer Act (FRB Regulation E) and the Expedited Funds Availability Act (FRB Regulation CC) for deposit activities?

CONTINGENCY PLANS

55. Have written contingency plans been developed and tested for partial or complete failure of each retail EFT system and/or communication lines between the institution, networks, and data center? Are the plans reasonably comprehensive in relation to the volume and importance of the specific Retail EFT activity to the institution's operation? At a minimum, do they provide for satisfactory store and forward procedures to protect against loss or duplication of data and for full recovery within a reasonable time period?

OTHER

56. Is there an internal control risk assessment (per FDICIA 112)? Assess its adequacy.

57. Is each individual site providing retail EFT services periodically reviewed by management to ensure policies and procedures, security measures, and equipment maintenance requirements are being adhered to?

58. If vendors are employed to perform any major services related to Retail EFT activities, are annual financial statements received and reviewed; and are reports covering audits of the vendors periodically obtained and reviewed?

59. Proceed to step 10, Tier 1.

Examiner | Date

_____|_____

Reviewer's Initials